Memorandum of Understanding between the Information Commissioner and the National Data Guardian for Health and Social Care

Introduction

1. This Memorandum of Understanding (MoU) establishes a framework for cooperation and information sharing between the Information Commissioner (**"the Commissioner"**) and the National Data Guardian for Health and Social Care (**"the NDG"**), collectively referred to as **"the parties"** throughout this document. In particular, it sets out the broad principles of collaboration and the legal framework governing the sharing of relevant information and intelligence between the parties. The shared aims of this MoU are to enable closer working between the parties, including the exchange of appropriate information, so as to assist them in discharging their regulatory and/or statutory functions.

2. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the Commissioner or the NDG. The parties have determined that they do not exchange sufficient quantities of personal data to warrant entering into a separate data sharing agreement, but this will be kept under review.

The role and function of the Information Commissioner

3. The Commissioner is a corporation sole appointed by Her Majesty the Queen under the General Data Protection Regulation and the Data Protection Act 2018 to act as the UK's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

4. The Commissioner is empowered to take a range of regulatory action for breaches of the following legislation:

   - Data Protection Act 2018 (DPA);
   - General Data Protection Regulation (GDPR);

- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR);
- Freedom of Information Act 2000 (FOIA);
- Environmental Information Regulations 2004 (EIR);
- Environmental Protection Public Sector Information Regulations 2009 (INSPIRE Regulations);
- Investigatory Powers Act 2016;
- Re-use of Public Sector Information Regulations 2015;
- Enterprise Act 2002;
- Security of Network and Information Systems Directive (NIS Directive); and
- Electronic Identification, Authentication and Trust Services Regulation (eIDAS).

5. Article 57 of the GDPR and Section 115(2)(a) of the DPA 2018 place a broad range of statutory duties on the Commissioner, including monitoring and enforcement of the GDPR, promotion of good practice and adherence to the data protection obligations by those who process personal data. These duties sit alongside those relating to the other enforcement regimes outlined in paragraph 4 above.

6. The Commissioner's regulatory and enforcement powers include:

- conducting assessments of compliance with the DPA, GDPR, PECR, eIDAS, the NIS Directive, FOIA and EIR;
- issuing information notices requiring individuals, controllers or processors to provide information in relation to an investigation;
- issuing enforcement notices, warnings, reprimands, practice recommendations and other orders requiring specific actions by an individual or organisation to resolve breaches (including potential breaches) of data protection legislation and other information rights obligations;

- administering fines by way of penalty notices in the circumstances set out in section 155 of the DPA;
- administering fixed penalties for failing to meet specific obligations (such as failing to pay the relevant fee to the Commissioner);
- issuing decision notices detailing the outcome of an investigation under FOIA or EIR;
- certifying contempt of court should an authority fail to comply with an information notice, decision notice or enforcement notice under FOIA or EIR; and
- prosecuting criminal offences before the Courts.

7. Regulation 31 of PECR, as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, also provides the Commissioner with the power to serve enforcement notices and issue monetary penalty notices as above to organisations which breach PECR. This includes, but is not limited to, breaches in the form of unsolicited marketing which falls within the ambit of PECR, including automated telephone calls made without consent, live telephone calls which have not been screened against the Telephone Preference Service, and unsolicited electronic messages (Regulations 19, 21 and 22 of PECR respectively).

The role and function of the National Data Guardian for Health and Social Care

8. The NDG is a statutory office holder appointed by the Secretary of State under the Health and Social Care (National Data Guardian) Act 2018 to act as an advocate for patients and service users on how their health and care data is used and to promote the provision of advice and guidance about the processing of health and adult social care data in England.

9. Health and adult social care data is defined in the Health and Social Care (National Data Guardian) Act 2018 as information that relates to the physical or mental health or condition of an individual, the diagnosis of his or her condition or his or her care or treatment, adult social care provided to an individual (or an assessment for such care), adult carer support provided to an individual (or an assessment for such support) whether or not the

identity of the individual is ascertainable or is to any extent derived, directly or indirectly from such information.

10. The NDG may publish guidance, and give advice, assistance and information, about the processing of health and adult social care data in England.

11. The Health and Social Care (National Data Guardian) Act 2018 imposes a duty on public bodies within the health and adult social care sector (and private organisations which contract with them to deliver health or adult social care services) to have regard to the NDG's published guidance that is relevant to those bodies or activities.

Purpose of information sharing

12. The purpose of the MoU is to enable the parties to share relevant information which enhances their ability to exercise their respective functions.

13. This MoU should not be interpreted as imposing a requirement on either party to disclose information in circumstances where doing so would breach their statutory responsibilities. In particular, each party must ensure that any disclosure of personal data pursuant to these arrangements fully complies with both the GDPR and the DPA 2018. The MoU sets out the potential legal basis for information sharing, but it is for each party to determine for themselves that any proposed disclosure is compliant with the law.

Principles of cooperation and sharing

14. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at her discretion, the NDG will alert the Commissioner to any potential breaches of the legislation regulated by the Commissioner, within the context of this relationship, discovered whilst undertaking the NDG's duties, and provide relevant and necessary supporting information.

15. Subject to any legal restrictions on the disclosure of information, the Commissioner will, at her discretion, share with the NDG information which falls within the scope of the NDG within the

context of this relationship and provide relevant and necessary supporting information.

16. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at their discretion, the parties will:

- Communicate regularly to discuss matters of mutual interest (this may involve participating in multi-agency groups to address common issues and threats); and
- Consult one another on any issues which might have significant implications for the other organisation.

17. The parties will comply with the general laws they are subject to, including, but not limited to, local data protection laws; the maintenance of any prescribed documentation and policies; and comply with any governance requirements in particular relating to security and retention, and process personal data in accordance with the statutory rights of individuals.

Lawful basis for sharing information

Information shared by the NDG with the Commissioner

18. The NDG, during the course of her activities, will receive information from a range of sources, including personal data. She will process all personal data in accordance with the principles of the GDPR, the DPA 2018 and the legislative framework in relation to health and social care information.

19. The Commissioner's statutory function relates to the legislation set out at paragraph 4, and this MoU governs information shared by the NDG to assist the Commissioner to meet those responsibilities. To the extent that any such shared information is to comprise personal data, as defined under the GDPR and DPA 2018, the NDG is a Controller so must ensure that she has a lawful basis to share it and that doing so would otherwise be compliant with the data protection principles. It must also ensure that sharing the information in question is consistent with its legal powers.

20. Section 131 of the Data Protection Act 2018 may both the lawful basis, from a data protection perspective, and the legal power for

the NDG to share information with the Commissioner. Under this particular provision, the NDG is not prohibited or restricted from disclosing information to the Commissioner by any other enactment or rule of law provided it is *"information necessary for the discharge of the Commissioner's functions"*.

Information shared by the Commissioner with the NDG

21. The Commissioner, during the course of her activities, will receive information from a range of sources, including personal data. She will process all personal data in accordance with the principles of the GDPR, the DPA 2018 and all other applicable legislation. The Commissioner may identify that information she holds, which may include personal data, ought to be shared with the NDG as it would assist her in performing her functions and responsibilities.

22. Section 132(1) of the DPA 2018 states that the Commissioner can only share confidential information with others if there is lawful authority to do so. In this context, the information will be considered confidential if has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, discharging her functions and it relates to an identifiable individual or business, and is not otherwise available to the public from other sources. This therefore includes, but is not limited to, personal data. Section 132(2) of the DPA 2018 sets out the circumstances in which the Commissioner will have the lawful authority to share that personal data with the NDG. In particular, it will be lawful in circumstances where:

- The sharing was necessary for the purpose of the Commissioner discharging her functions (section 132(2)(c));
- The sharing was made for the purposes of criminal or civil proceedings, however arising (section 132(2)(e)); or
- The sharing was necessary in the public interest, taking into account the rights, freedoms and legitimate interests of any person (section 132(2)(f)).

23. The Commissioner will therefore be permitted to share information with the NDG in circumstances where she has determined that it is reasonably necessary to do so in furtherance of one of those

grounds outlined at paragraph 22. In doing so, the Commissioner will identify the function of the NDG with which that information may assist, and assess whether that function could reasonably be achieved without access to the particular information in question. In particular, where the information proposed for sharing with the NDG amounts to personal data the Commissioner will consider whether it is necessary to provide it in an identifiable form in order for the NDG to perform her functions, or whether disclosing it in an anonymised form would suffice.

24. If information to be disclosed by the Commissioner was received by her in the course of discharging her functions as a designated enforcer under the Enterprise Act 2002, any disclosure shall be made in accordance with the restrictions set out in Part 9 of that Act.

25. Where information is to be disclosed by either party for law enforcement purposes under section 35(4) or (5) of the DPA 2018 then they will only do so in accordance with an appropriate policy document as outlined by section 42 of the DPA.

26. Where a request for information is received by either party under data protection laws, FOIA or EIR, and where the information being sought under that request includes information obtained from, or shared by, the other party, the recipient of the request will seek the views of the other party. In particular, the receiving party will have regard to the FOIA section 45 Code of Practice and/or the EIR Regulation 16 Code of Practice, as appropriate. However the decision to disclose or withhold the information (and therefore any liability arising out of that decision) remains with the party in receipt of the request as Controller in respect of that data.

Method of exchange

27. Appropriate security measures shall be agreed to protect information transfers in accordance with the sensitivity of the information and any classification that is applied by the sender.

Confidentiality and data breach reporting

28. Where confidential material is shared between the parties it will be marked with the appropriate security classification.

29. Where one party has received information from the other, it will consult with the other party before passing the information to a third party or using the information in an enforcement proceeding or court case.

30. Where confidential material obtained from, or shared by, the originating party is wrongfully disclosed by the party holding the information, this party will bring this to the attention of the originating party without delay. This is in addition to obligations to report a personal data breach under the GDPR and/or DPA where personal data is contained in the information disclosed.

Duration and review of the MoU

31. The parties will monitor the operation of this MoU and will review it biennially.

32. Any minor changes to this memorandum identified between reviews may be agreed in writing between the parties.

33. Any issues arising in relation to this memorandum will be notified to the point of contact for each organisation.

Key contacts

34. The parties have both identified a key person who is responsible for managing this MoU:

35.

Information Commissioner's Office	**Office of the National Data Guardian**
[redacted] Address: Wycliffe House, Water Lane, Wilmslow, SK9 5AF	[redacted] Address: 1 Trevelyan Square, Boar Lane, Leeds, LS1 6AE

36. Those individuals will maintain an open dialogue between each other in order to ensure that the MoU remains effective and fit for purpose. They will also seek to identify any difficulties in the working relationship, and proactively seek to minimise the same.

Signatories

Deputy Commissioner ICO	
[redacted] Date: 15/01/2020	[redacted] Date: 24.2.20